US005485409A

United States Patent [19]

Gupta et al.

[11] **Patent Number: 5,485,409**

[45] **Date of Patent: Jan. 16, 1996**

[54] **AUTOMATED PENETRATION ANALYSIS SYSTEM AND METHOD**

[75] Inventors: **Sarbari Gupta**, Rockville; **Virgil D. Gligor**, Chevy Chase, both of Md.

[73] Assignee: **International Business Machines Corporation**, Armonk, N.Y.

[21] Appl. No.: **875,945**

[22] Filed: **Apr. 30, 1992**

[51] **Int. Cl.**^{6} **H04L 9/00; G06F 13/00**

[52] **U.S. Cl.** **395/186**; 364/DIG. 1; 364/286.4; 364/DIG. 2; 364/918.7; 395/600; 380/4

[58] **Field of Search** 364/580, 570, 364/918.7, 949.81, 286.4, 286.5, 286.6, 419; 395/50, 51, 61, 911, 912, 913, 914, 915, 916, 917, 918, 725; 340/825.31, 825.34; 380/4

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,649,515	3/1987	Thompson et al.	395/911 X
4,956,769	9/1990	Smith	364/200
5,060,279	10/1991	Crawford et al.	395/911 X
5,099,436	3/1992	McCown et al.	395/911 X
5,133,063	7/1992	Naito et al.	395/50 X
5,161,245	11/1992	Fenwick	364/419 X
5,197,004	3/1993	Sobotka et al.	364/419

OTHER PUBLICATIONS

Gupta et al., "Towards a Theory of Penetration–Resistant Systems and its Applications", Proc. of the 4th IEEE Workshop on Computer Security Foundations, Franconia, N.H., pp. 62–78, Jun. 1991.

Jiang et al., "Distributed System Security Research at FSD Gaithersburg", IBM Document No. FSDSS–9202, Jan. 8, 1992.

Gupta et al., "Experience with a Penetartion Analysis Method and Tool", U of MD, Electrical Engineering Department, Technical Report No. 2881, Apr. 1992.

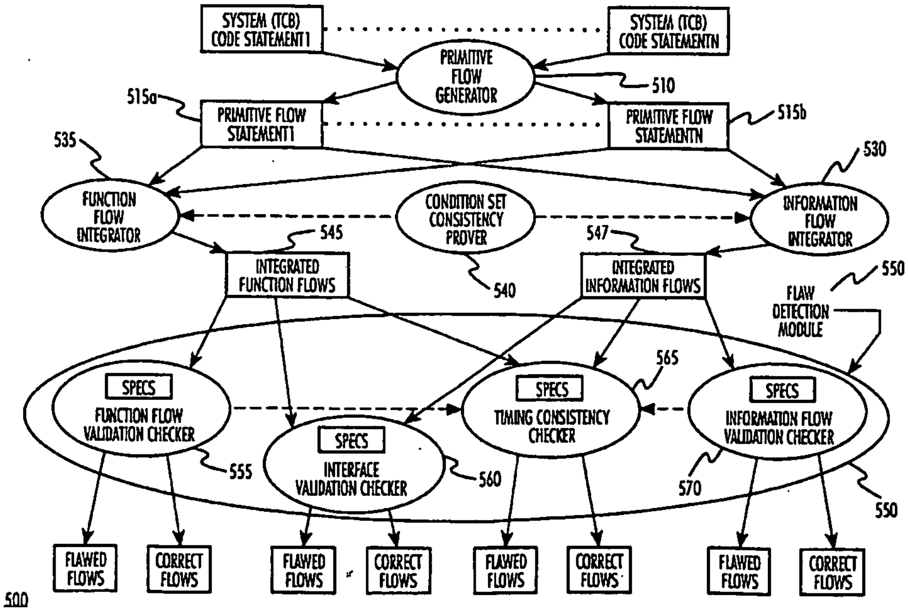
Tsai et al., "Distributed System and Security Management with Centralized Control", 1992 EurOpen/USENIX Workshop, Jersey, U.K., Apr. 6–9, 1992.

Primary Examiner—Emanuel T. Voeltz
Assistant Examiner—Eric W. Stamber
Attorney, Agent, or Firm—Sterne, Kessler, Goldstein & Fox

[57] **ABSTRACT**

The present invention provides a penetration-analysis method, which (1) provides a systematic approach to penetration analysis, (2) enables the verification of penetration-resistance properties, and (3) is amenable to automation. An Automated Penetration Analysis (APA) tool is provided, to support the penetration analysis method. The penetration-analysis system and method is based on a theory of penetration-resistant computer systems, a model of penetration analysis, and a unified representation of penetration patterns. The theory consists of the Hypothesis of Penetration-Resistant Systems and a set of design properties that characterize resistance to penetration. The penetration-analysis model defines a set of states, a state-invariant for penetration resistance, and a set of rules that can be applied for analyzing the penetration vulnerability of a system. An interpretation of the Hypothesis of Penetration-Resistant Systems within a given system provides the Hypothesis of Penetration Patterns, which enables the present invention to define a unified representation for a large set of penetration instances as missing check patterns.

6 Claims, 31 Drawing Sheets


SYSTEM (TCB) CODE STATEMENT1
SYSTEM (TCB) CODE STATEMENTN
PRIMITIVE FLOW GENERATOR
510
515a
PRIMITIVE FLOW STATEMENT1
PRIMITIVE FLOW STATEMENTN
515b
535
530
FUNCTION FLOW INTEGRATOR
CONDITION SET CONSISTENCY PROVER
INFORMATION FLOW INTEGRATOR
545
547
INTEGRATED FUNCTION FLOWS
540
INTEGRATED INFORMATION FLOWS
550
FLAW DETECTION MODULE
565
SPECS
FUNCTION FLOW VALIDATION CHECKER
SPECS
TIMING CONSISTENCY CHECKER
SPECS
INFORMATION FLOW VALIDATION CHECKER
SPECS
INTERFACE VALIDATION CHECKER
555
560
570
550
FLAWED FLOWS
CORRECT FLOWS
FLAWED FLOWS
CORRECT FLOWS
FLAWED FLOWS
CORRECT FLOWS
FLAWED FLOWS
CORRECT FLOWS
500